Responded to a Scam?
Take These Steps

Email and phone scams are becoming increasingly sophisticated, which may make it difficult to identify whether a message is legitimate or trying to trick you into releasing personal information.

Shared a Password?
If you do fall victim to a scam and shared personal information, like your password, we recommend that you change the passwords to your online accounts immediately. You should also update your software and run a virus scan.

Shared Financial Information?
If you responded to a scam and shared financial information, such as your bank account number, contact the Rowan University Department of Public Safety at 856-256-4922 and ask to speak or meet with a police officer so they can file a report.

We also recommend you change your passwords, update your software, check your accounts regularly, contact credit agencies, banks, credit card companies and other agencies. For details, review our What to Do If You Responded to an Email or Phone Scam article.
Help Us Keep Rowan University Safe

We rely on every member of Rowan University to learn and follow best practices for staying safe online. Use these tips to get started, and visit go.rowan.edu/ncsam for more information.

**Lock Down Your Login**

Your usernames and passwords are not enough to protect key accounts. Use strong authentication tools whenever offered.

**Keep a Clean Machine**

Keep all software on internet-connected devices current to reduce risk of infection from ransomware and malware.

**When in Doubt, Throw it Out**

If an email, tweet or other post looks suspicious, even if you know the source, it's best to delete or, if appropriate, mark it as junk.

**Back It Up**

Protect your valuable work, music, photos and other digital information by making an electronic copy and storing it safely.

**Own Your Online Presence**

Set the privacy and security settings on websites to your comfort level for information sharing. It is OK to limit information you share online.

**Share With Care**

Think before posting about yourself and others online. Consider what a post reveals, who might see it and how it might affect you or others.

**Value Personal Information**

Information about you, such as purchase history or location, has value — just like money. Be thoughtful about who gets that information.
Security Threats

In August, we detected and blocked 50 virus attacks and 44,500 emails with malicious URLs sent to our network.

Universities are prime targets for cyberattacks due to the amount of personal data and sensitive research material stored on their networks.

Please immediately contact the Technology Support Center if you think you have clicked on a malicious link or attachment in an email. Acting quickly will minimize the risk to the University.